Autocorrelation and Linear Complexity of Quaternary Sequences of Period $2p$ Based on Cyclotomic Classes of Order Four

Vladimir Edemskiy and Andrew Ivanov
Department of Applied Mathematics and Computer Science
Novgorod State University
Veliky Novgorod, Russia
Email: Vladimir.Edemsky@novsu.ru, dk@live.ru

***Abstract*—We examine the linear complexity and the autocorrelation properties of new quaternary cyclotomic sequences of period $2p$. The sequences are constructed via the cyclotomic classes of order four.**

I. Introduction

The periodic autocorrelation function and the linear complexity are the important merits for sequence design. The autocorrelation measures the amount of similarity between the sequence S and a shift of S by w positions. The linear complexity (L) is defined as the length of the shortest linear-feedback-shift register that can generate the sequence [1]. Large linear complexity and and small autocorrelation for all $w, 1 \leq w \leq N-1$, where N is a period of a sequence, are desirable features for sequences used in applications like cryptology and other (see [1], [12], [13]). Binary and quaternary sequences are the subjects of interest [11], [10].

Use of classical cyclotomic classes and generalized cyclotomic classes to construct sequences, which are called classical cyclotomic sequences and generalized cyclotomic sequences respectively, is an important method for sequence design [1]. Legendre sequences are based on cyclotomic classes of order two. The properties of Legendre sequences are well known [3]. Kim et al. [9] defined new quaternary cyclotomic sequences of length $2p$, where p is an odd prime, and derived the autocorrelation function of these sequences (see also [4]). Their design is based on generalized cyclotomic classes of order two. This approach was further developed in [8] for sequences of length $2p^m$.

Ding et al. [2] considered the sequences based on cyclotomic classes of order four and gave several new families of binary sequences of period $2p$ with optimal three-level autocorrelation. Now it is interesting to see is it possible to find quaternary sequences of length $2p$ based on cyclotomic classes of order four with desirable properties using the method from [2], [9].

First, we recall shortly the design of sequences from [2]. Let $p = 4R+1$ be a prime, where R is a natural number, and let g be a primitive root modulo p. Put, by definition

$$H_k = \{g^{k+4t} (\mathrm{mod} p),\ t = 0, 1, \ldots, R-1\}, \quad k = 0, 1, 2, 3.$$

Then H_k are called cyclotomic classes of order 4 [1].

By the Chinese Remainder Theorem, $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ relatively to isomorphism $f(w) = (w_1, w_2)$, where $w_1 = w \,(\mathrm{mod}\ 2)$, $w_2 = w \ (\mathrm{mod}\ p)$. Here and hereafter $a(\mathrm{mod}\ p)$ denotes the least nonnegative integer that is congruent to a modulo p.

Let $C_k = \{0\} \times H_{j_k} \cup \{1\} \times H_{l_k}$, where $0 \leq j_k, l_k \leq 3$ and $j_k \neq j_m, l_k \neq l_m$ then $k \neq m, k, m = 0, 1, 2, 3$. The quaternary sequence $\{s(t)\}$ is defined as

$$s(t) = \begin{cases} k, & \text{if } t(\mathrm{mod}\ 2p) \in C_k, \\ 0, & \text{if } t \equiv 0 (\mathrm{mod}\ 2p), \\ 2, & \text{if } t \equiv p (\mathrm{mod}\ 2p). \end{cases} \tag{1}$$

This is a generalization of the construction proposed in [2] and [9] to build binary and quaternary sequences, respectively. In the next sections we derive the periodic autocorrelation function of $s(t)$; we also determine the linear complexity of $s(t)$ over the finite field of four elements and over the finite ring of order four.

II. Autocorrelation

The autocorrelation of $2p$-periodic sequence $s(t)$ is a complex-valued function defined by

$$R(w) = \sum_{n=0}^{2p-1} i^{s(n)-s(n+w)},$$

where $i = \sqrt{-1}$ is an imaginary unit.

Let $v(t) = i^{s(t)}$. Then, the periodic autocorrelation function at shift w of $\{s(t)\}$ is given by

$$R(w) = \sum_{n=0}^{2p-1} v(n) v^*(n+w), \tag{2}$$

where $v^*(t)$ is the complex conjugate of $v(t)$.

Let D, E be a subset of ring $\mathbb{Z}_{2p}$. By definition, a difference function $d_w(F, E)$ can by written as

$$d_w(F, E) = |F \cap (E + w)|,$$

where $E + w$ denotes the set $\{w + e : e \in E\}$ and " $+$ " denotes an addition modulo $2p$.

It is well known that if $f(t)$ and $e(t)$ are the characteristic sequences of F and E, i.e.,

$$f(t) = \begin{cases} 1, & \text{if } t(\mathrm{mod} 2p) \in F, \\ 0, & \text{otherwise.} \end{cases}$$

and

$$e(t) = \begin{cases} 1, & \text{if } t(\mathrm{mod} 2p) \in E, \\ 0, & \text{otherwise.} \end{cases}$$

then

$$\sum_{j=0}^{2p-1} f(t)e(t+w) = d_w(F,E). \quad (3)$$

Consequently, by (1) - (3) for real $\big(\mathrm{ReR(w)}\big)$ and imaginary $\big(\mathrm{ImR(w)}\big)$ parts of the autocorrelation function $R(w)$ we have the following equations:

$$\begin{aligned} &\mathrm{Re}R(w) = d_w(C_0+0, C_0+0) + d_w(C_1, C_1) \\ &+ d_w(C_2+p, C_2+p) + d_w(C_3, C_3) - d_w(C_0+0, C_2+p) \\ &- d_w(C_2+p, C_0+0) - d_w(C_1, C_3) - d_w(C_3, C_1), \quad (4) \end{aligned}$$

and

$$\begin{aligned} &\mathrm{Im}R(S,w) = d_w(C_1, C_0+0) + d_w(C_3, C_2+p) \\ &+ d_w(C_0+0, C_3) + d_w(C_2+p, C_1) - d_w(C_1, C_2+p) \\ &- d_w(C_3, C_0+0) - d_w(C_0+0, C_1) - d_w(C_2+p, C_3). \quad (5) \end{aligned}$$

So, in order to obtain $R(w)$ it is sufficient to find difference functions listed in (4) - (5).

Suppose that F_0, F_1, E_0, E_1 are subsets of $\mathbb{Z}_p$.

Lemma 1: Let $F = \{0\} \times F_0 \cup \{1\} \times F_1$, and $E = \{0\} \times E_0 \cup \{1\} \times E_1$, and $w = (w_0, w_1) \in \mathbb{Z}_2 \times \mathbb{Z}_p$. Then

$$d_w(F,E) = \begin{cases} |F_0 \cap E_0| + |F_1 \cap E_1|, & \text{if } w = 0, \\ |F_0 \cap (E_0 + w_1)| + |F_1 \cap (E_1 + w_1)|, & \\ \qquad\qquad \text{if } w_0 = 0, w_1 \neq 0, & \\ |F_0 \cap (E_1 + w_1)| + |F_1 \cap (E_0 + w_1)|, & \\ \qquad\qquad \text{if } w_0 = 0, w_1 \neq 0, & \\ |F_0 \cap E_1| + |F_1 \cap E_0|, & \text{if } w = p. \end{cases}$$

Proof: For the case $F = E$ Lemma 1 was proved in [2]. When $F \neq E$ it is proved similarly. ■

To derive difference functions we will need cyclotomic numbers. Recall that the cyclotomic numbers of order 4 in this case are defined as [7]

$$(i,j) = |(H_i + 1) \cap H_j|.$$

Note that every prime $p \equiv 1(\mathrm{mod}\ 4)$ has a quadratic partition $p = x^2 + 4y^2$, where $x, y \in \mathbb{Z}$ and $x \equiv 1(\mathrm{mod}\ 4)$. It is well known how to express cyclotomic numbers over the values of p, x, y [7]. Here y is two-valued, depending on the choice of the primitive root g employed to define the cyclotomic classes.

Lemma 2: If $u \in H_h$, $h = 0, 1, 2, 3$, then

(i) $|H_j \cap (H_l + u)| = (h - l, j - l)$,

(ii) $|H_j \cap \{u\}| = \begin{cases} 1, & \text{if } h = j, \\ 0, & \text{otherwise.} \end{cases}$

(iii) $|\{0\} \cap (H_j + u)| =$

$$\begin{cases} 1, & \text{if } h = j \text{ and } p \equiv 1 \pmod 8 \\ & \quad \text{or} \quad h \equiv (j+2) (\mathrm{mod}\ 4) \ \text{ and } \ p \equiv 5 \pmod 8, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Notice that

$$|H_j \cap (H_l + u)| = |u^{-1} H_j \cap (u^{-1} H_l + 1)|.$$

Then $|H_j \cap (H_l + u)| = (l - h, j - h)$, and since $(l - h, j - h) = (h - l, j - l)$ [7], then the first statement is proved. The second statement of Lemma 2 is obvious.

Subsequently, since $-1 = g^{(p-1)/2}$, then $-1 \in H_0$ for $p \equiv 1 \pmod 8$ and $-1 \in H_2$ for $p \equiv 5 \pmod 8$. Hence, if $u \in H_h$, then $-u \in H_h$ for $p \equiv 1 \pmod 8$ and $-u \in H_{(h+2)(\mathrm{mod}\ 4)}$ for $p \equiv 5 \pmod 8$. From this follows the third statement of Lemma 2. ■

By Lemmas 1- 2 and formulas (4)-(5) we can derive autocorrelation of $\{s(t)\}$ defined by (1). Note that the set of values $R(w), w \neq 0$ do not vary under the complex conjugation of the sequence and under the cyclic shift modulo four of cyclotomic classes numbers in (1). Therefore, it is enough to consider two options, namely when the vector (j_0, j_1, j_2, j_3) equals $(0, 1, 2, 3)$ or $(0, 2, 1, 3)$. Consider examples of finding the autocorrelation function for every option.

For the sake of convenience let us denote $\{k\} \times H_l, k = 0, 1, l = 0, 1, 2, 3$ as $H_{k,l}$.

Consider the quaternary sequence $\{s(t)\}$ defined as

$$s(t) = \begin{cases} 0, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{0\} \cup H_{0,0} \cup H_{1,1}, \\ 1, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,1} \cup H_{1,2}, \\ 2, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{p\} \cup H_{0,2} \cup H_{1,3}, \\ 3, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,3} \cup H_{1,0}. \end{cases} \quad (6)$$

Theorem 3: Let the quaternary sequence $\{s(t)\}$ be defined by (6). Then

(i) $R(w) \in \{-2 \pm 2i, \pm 2i, -2\}, w = 1, \ldots, 2p-1$, if $p \equiv 5 \pmod 8$,

(ii) $R(w) \in \{-4, \pm 2, 0\}, w = 1, \ldots, 2p-1$, if $p \equiv 1 \pmod 8$.

Proof: As before, let $w = (w_0, w_1)$. Consider several options.

1) Let $w_0 = 0, w_1 \neq 0$. If $w_1 \in H_h, h = 0, 1, 2, 3$ then by (4), Lemma 1 and Lemma 2 we have

$$\mathrm{Re}R(w) = 2 \sum_{k=0}^{3} \big((h-k, 0) - (h-k, 2)\big) + \delta,$$

where

$$\delta = \begin{cases} 0, & \text{if } \ \mathrm{p} \equiv 5 (\mathrm{mod}\ 8), \\ 2, & \text{if } \ p \equiv 1 (\mathrm{mod}\ 8) \ \text{ and } \ h = 0, 3, \\ -2, & \text{if } \ p \equiv 1 (\mathrm{mod}\ 8) \ \text{ and } \ h = 1, 2. \end{cases}$$

It is shown [7] that

$$\sum_{k=0}^{3} (h-k, 0) - (h-k, 2) = \sum_{j=0}^{3} (j, 0) - \sum_{j=0}^{3} (j, 2) = -1,$$

hence, if $w_0 = 0, w_1 \neq 0$ and $w_1 \in H_h$ then

$$\mathrm{Re}R(w) = \begin{cases} -2, & \text{if } \ \mathrm{p} \equiv 5(\mathrm{mod}\ 8), \\ 0, & \text{if } \ p \equiv 1(\mathrm{mod}\ 8) \ \text{ and } \ h = 0, 3, \\ -4, & \text{if } \ p \equiv 1(\mathrm{mod}\ 8) \ \text{ and } \ h = 1, 2. \end{cases}$$

Similarly we obtain

$$\mathrm{Im}R(w) = \begin{cases} 2i, & \text{if } \ p \equiv 5(\mathrm{mod}\ 8) \ \text{ and } \ h = 0, 1, \\ -2i, & \text{if } \ p \equiv 5(\mathrm{mod}\ 8) \ \text{ and } \ h = 2, 3, \\ 0, & \text{if } \ p \equiv 1(\mathrm{mod}\ 8). \end{cases}$$

2) Let $w_0 = 1, w_0 \neq 0$. Here, by Lemmas 1 and 2

$$R(w) = \begin{cases} 2, & \text{if } \ p \equiv 5(\mathrm{mod}\ 8) \\ -2, & \text{if } \ p \equiv 1(\mathrm{mod}\ 8). \end{cases}$$

3) Let $w_0 = 1, w_1 \neq 0$. As before, it can easily be checked that

$$R(w) = \begin{cases} 2i, & \text{if } \ p \equiv 5(\mathrm{mod}\ 8) \ \text{ and } \ h = 0, 3 \\ & \quad \text{or } \ p \equiv 1(\mathrm{mod}\ 8) \ \text{ and } \ h = 0, 1, \\ -2i, & \text{if } \ p \equiv 5(\mathrm{mod}\ 8) \ \text{ and } \ h = 1, 2, \\ & \quad \text{or } \ p \equiv 1(\mathrm{mod}\ 8) \ \text{ and } \ h = 2, 3. \end{cases}$$

Theorem 3 is proved. ■

Note that if we take $s(0) = s(p) = 0$ then under the conditions of theorem 3 we obtain $|R(w)| = 2, w = 1, \ldots, 2p-1$.

If the quaternary sequence $\{s(t)\}$ is defined as

$$s(t) = \begin{cases} 0, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{0\} \cup H_{0,0} \cup H_{1,2}, \\ 1, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,2} \cup H_{1,0}, \\ 2, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{p\} \cup H_{0,1} \cup H_{1,3}, \\ 3, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,3} \cup H_{1,1}, \end{cases} \tag{7}$$

then we can similarly derive the following lemma.

Lemma 4: Let the quaternary sequence $\{s(t)\}$ defined by (7) and $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then

(i) $\max_{w \neq 0} |R(w)| = \max |-2 \pm 2y \pm 2i|$, if $p \equiv 5\ (\mathrm{mod}\ 8)$,

(ii) $\max_{w \neq 0} |R(w)| = \max |-4 \pm 2y|$, if $p \equiv 1\ (\mathrm{mod} 8)$.

Autocorrelation of new sequences is better than of the quaternary sequences proposed by Kim et al.

Under the conditions of Lemma 4 the autocorrelation properties of $\{s(t)\}$ are worse than under the conditions of Theorem 3. Moreover, we can show that if the sequence is constructed by (1) then its autocorrelation can't be better that under the conditions of Theorem 3.

Further, we derive the linear complexity of $\{s(t)\}$. On the one hand, it is possible to derive the linear complexity of quaternary sequences over the finite ring $\mathbb{Z}_4$. An alternative approach is Gray-mapping the quaternary sequences and obtain the sequences defined over $\mathbb{F}_4$ (the finite field of 4 elements). Generally, these two ways lead to different values for the linear complexity because arithmetics of $\mathbb{F}_4$ and $\mathbb{Z}_4$ differ, see for example [6].

We explore the linear complexity of $\{s(t)\}$ for both alternatives.

III. The Linear Complexity of Quaternary Sequences over the Finite Field of Order 4

We can convert quaternary sequences into the sequences of elements belonging to the finite field of order four by using Gray map. In this section we demonstrate that as a result of Gray mapping of the sequences with good autocorrelation properties from the Section II we obtain the sequences with high linear complexity over the finite field of order four.

Let $\mathbb{F}_4 = \{0, 1, \mu, \mu+1\}$ be a finite field of four elements, and let $\varphi(a)$ be a Gray map defined by $\varphi(0) = (0,\ 0)$, $\varphi(1) = (0,\ 1)$, $\varphi(2) = (1,\ 1)$, $\varphi(3) = (1,\ 0)$. Suppose $\{s(t)\}$ is constructed by (6). Consider $\mathbb{F}_4$ as a vector space over $\mathbb{F}_2$ with basis $\mu,\ 1$. Denote Gray-mapping of $\{s(t)\}$ as $\{u(t)\}$, i.e.,

$$u(t) = \begin{cases} 0, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{0\} \cup H_{0,0} \cup H_{1,1}, \\ 1, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,1} \cup H_{1,2}, \\ \mu+1, & \text{if } \ t(\mathrm{mod}\ 2p) \in \{p\} \cup H_{0,2} \cup H_{1,3}, \\ \mu, & \text{if } \ t(\mathrm{mod}\ 2p) \in H_{0,3} \cup H_{1,0}. \end{cases} \tag{8}$$

It is well known (see [1]) that the minimal polynomial and the linear complexity of sequence can be derived as follows:

$$L = N - \deg\big(\gcd\left(x^N - 1, U(x)\right)\big), \qquad m(x) = \left(x^N - 1\right) / \gcd\left(x^N - 1, U(x)\right), \tag{9}$$

here $U(x) = \sum_{t=0}^{N-1} u(t) x^t$.

For $N = 2p$ we can write (9) in the form

$$L = 2p - \deg \gcd\big((x^p - 1)^2, U(x)\big) \tag{10}$$

Let α denote a primitive root of unity of order p in the extension of the field F_4. From (10) it follows that to derive the linear complexity and the minimal polynomial of $\{u(t)\}$ it is sufficient to determine the number of roots and multiple roots of $U(x)$ in the set $\{\alpha^v, v = 0, 1, ..., p-1\}$.

Now we introduce auxiliary polynomials. Let $U_4(x) = \sum_{i \in H_0} x^i$ and $U_2(x) = \sum_{i \in H_0 \cup H_2} x^i$. The properties of $U_2(x)$ and $U_4(x)$ were examined in [3] and [5], respectively.

Lemma 5: If $v = 0, \ldots, p-1$ then
$\sum_{v \in H_{0,k}} \alpha^v = \sum_{v \in H_{1,k}} \alpha^v = U_4(\alpha^{g^k})$.

Proof: By definition

$$\{a(\mathrm{mod}\ p) | a \in H_{k,l}\} = H_l$$

for all $k = 0, 1; l = 0, 1, 2, 3$. Since $g^l H_0 = H_l$, then $\sum_{j \in H_{k,l}} \alpha^j = \sum_{j \in H_0} \alpha^{g^k j}$. Lemma 5 follows from the last equality. ■

By Lemma 5 and by the definitions of the auxiliary polynomials we have

$$U_4(\alpha^v) + U_4(\alpha^{vg^2}) = U_2(\alpha^v) \tag{11}$$

Theorem 6: Let the sequence $\{u(t)\}$ be constructed by (8). Then

1. $L = 2p$ and $m(x) = x^{2p} - 1$, if $p \equiv 1(\mathrm{mod}\ 8)$,
2. $L = (3p+1)/2$ and $m(x) = (x^{2p} - 1)/H(x)$, here $H(x) = \prod_{i \in H_1 \bigcup H_3} (x - \alpha^i)$, if $p \equiv 5(\mathrm{mod}\ 8)$.

Proof: By definition, the polynomial of the sequence can be written as:

$$U(x)=\sum_{j\in H_{0,1}\cup H_{1,2}} x^j+(\mu+1)\sum_{j\in H_{0,2}\cup H_{1,3}} x^j + \mu\sum_{j\in H_{0,3}\cup H_{1,0}} x^j+(\mu+1)x^p.$$

The number of the elements in each of the three sums is even, then $U(1)=\mu+1$.

Further, by Lemma 5 we have

$$U(\alpha^v)=\mu+1+U_4(\alpha^{gv})+U_4(\alpha^{g^2v}) +(\mu+1)\left(U_4(\alpha^{g^2v})+U_4(\alpha^{g^3v})\right)+\mu\left(U_4(\alpha^{g^3v})+S_4(\alpha^v)\right),$$

or to put it differently,

$$U(\alpha^v)=\mu+1+U_4(\alpha^{gv})+U_4(\alpha^{g^3v}) + \mu\left(U_4(\alpha^{g^2v})+U_4(\alpha^v)\right).$$

Now, by (11) we obtain

$$U(\alpha^v)=U_2(\alpha^{\theta v})+\mu U_2(\alpha^v)+\mu+1 \qquad (12)$$

Taking into account that $p\equiv 1(\mathrm{mod}\ 4)$, let us examine two options:

1. Let $p\equiv 1(\mathrm{mod}\ 8)$, then it was shown in [3] that with an appropriate choice of α we have

$$U_2(\alpha^v)=\begin{cases}1, & \text{if } v\in H_0\cup H_2,\\ 0, & \text{if } v\in H_1\cup H_3.\end{cases}$$

Therefore, $U(\alpha^v)\in\{1,\ \mu\}$, i.e., $U(\alpha^v)\neq 0$ when $v=0,1,...,p-1$, and the statement of Theorem 6 follows from (9) and (10).

2. Let $p\equiv 5(\mathrm{mod}\,8)$, then as shown in [3],

$$U_2(\alpha^v)=\begin{cases}\mu, & \text{if } v\in H_0\cup H_2,\\ \mu+1, & \text{if } v\in H_1\cup H_3.\end{cases}$$

Therefore, if $v\in H_0\cup H_2$ then by (12) $U(\alpha^v)=\mu+1$; if $v\in H_1\cup H_3$ then $U(\alpha^v)=0$.

Now we determine the multiplicity of the roots of the form α^v of the polynomial $U(x)$. The derivative of $U(x)$ is

$$U'(x)=\sum_{j\in H_{1,2}} x^{j-1}+(\mu+1)\sum_{j\in H_{1,3}} x^{j-1} + \mu\sum_{j\in H_{1,0}} x^{j-1}+(\mu+1)x^{p-1}.$$

Now,

$$U'(\alpha^v)=\alpha^{-v}\big(\mu+1+U_4(\alpha^{g^2v}) + (\mu+1)U_4(\alpha^{g^3v})+\mu U_4(\alpha^v)\big). \qquad (13)$$

If $p\equiv 5(\mathrm{mod}\,8)$ then $2\in H_1\cup H_3$. Thus, as shown in [4], if $v\in H_k$, then $U_4(\alpha^v)=\varsigma^{2^k}$ or $U_4(\alpha^v)=\varsigma^{2^{4-k}}$, here ς satisfies the conditions - $\varsigma^8+\varsigma^4+\varsigma^2+\varsigma=1$ and $\varsigma^4+\varsigma=\mu$ in the field $\mathbb{F}_4$.

So, from (13) we get $U'(\alpha^v)\neq 0$ for $v\in H_1\cup H_3$. Hence, we see that all the roots of $U(x)$ of the form α^v are simple and the statement of Theorem 6 for $p\equiv 5(\mathrm{mod}\,8)$ follows from (9) and (10). ■

If we apply Gray mapping to the sequence defined by (7), we obtain

$$b(t)=\begin{cases}0, & \text{if } t(\mathrm{mod}\ 2p)\in\{0\}\cup H_{0,0}\cup H_{1,2},\\ 1, & \text{if } t(\mathrm{mod}\ 2p)\in H_{0,2}\cup H_{1,0},\\ \mu+1, & \text{if } t(\mathrm{mod}\ 2p)\in\{p\}\cup H_{0,1}\cup H_{1,3},\\ \mu, & \text{if } t(\mathrm{mod}\ 2p)\in H_{0,3}\cup H_{1,1}.\end{cases} \qquad (14)$$

Lemma 7: Let the sequence $\{b(t)\}$ be constructed by (14). Then $L=2p$ and $m(x)=x^{2p}-1$.

Lemma 7 is proved in the same way as Theorem 6.

We can derive the linear complexity of the other sequences of period $2p$ by applying formulas for $U_4(\alpha^v)$ from [5].

IV. The Linear Complexity of Quaternary Sequences over the Ring of Order 4

A polynomial $C(x)=1+c_1x+...+c_mx^m$, $C(x)\in\mathbb{Z}_4[x]$ is called an associated connection polynomial of periodic sequence $\{s(t)\}$ over $\mathbb{Z}_4$, if coefficients $c_1,c_2,...,c_m$ satisfy $s(t)=-c_1s(t-1)-c_2s(t-2)-...-c_ms(t-m),\ \forall t\geq m$. The linear complexity of periodic sequence $\{s(t)\}$ over $\mathbb{Z}_4$ is equal to

$$L=\min\{\deg C(x)|\ \ C(x)\text{ is an associated connection polynomial of }\{s(t)\}\}.$$

Also, we can define L as the degree of the minimal polynomial.

We know that $C(x)$ is an associated connection polynomial of $\{s(t)\}$ if and only if

$$S(x)C(x)\equiv 0\ \ \big(\mathrm{mod}(x^{2p}-1)\big), \qquad (15)$$

where $S(x)=s(0)+s(1)x+...+s(2p-1)x^{2p-1}$ [15].

Let $R=GF(2^{2r},2^2)$ be Galois ring of characteristic 4, where r is the order of 2 modulo p [14]. The group of invertible elements $R^*=R\setminus 2R$ of the ring R contains the cyclic subgroup of order 2^r-1 [14]. Then, in R^* there must exist an element β of order p. Let $\gamma=3\beta$, then the order of γ is equal $2p$ and $\gamma^p=-1$.

The maximal ideal of the ring R is $2R$ [14]. Here we have the natural epimorphism of the rings R and $\overline{R}=R/2R$. Let $\overline{r}$ denote the image of the element $r\in R$ under this epimorphism.

Lemma 8: Let the sequence $\{s(t)\}$ be defined by (6). Then $\overline{S(\gamma^v)}=1$ if $v=1,\ldots,2p-1, v\neq p$.

Proof: By definition of γ it follows that $\overline{\gamma}^p=\overline{\gamma}$ and $\overline{\gamma}\neq 0,1$. Then $\sum_{j=1}^{p-1}\overline{\gamma}^j=1$ in the ring $\overline{R}$.

By (6) we have

$$S(x)=\sum_{j\in H_{0,1}\cup H_{1,2}} x^j+2\sum_{j\in H_{0,2}\cup H_{1,3}} x^j + 3\sum_{j\in H_{0,3}\cup H_{1,0}} x^j+2x^p.$$

In the same way as in Lemma 5 we obtain

$$\overline{S(\gamma^v)} = \sum_{j\in H_1} \overline{\gamma}^{jv} + \sum_{j\in H_2} \overline{\gamma}^{jv} + \sum_{j\in H_3} \overline{\gamma}^{jv} + \sum_{j\in H_0} \overline{\gamma}^{jv} = \sum_{l=1}^{p-1} \overline{\gamma}^{l} = 1.$$

■

Before proceeding to the main results of Section, we note that in the ring R the number of polynomial's roots can be greater than its degree. For example, if

$$P(x) = 2(x^p - 1)/(x - 1),$$

then $P(\gamma^v) = 0$ for $v = 1, \ldots, 2p-1, v \neq p$, but at the same time $P(x)$ is not divisible by the product $(x^{2p} - 1)/(x^2 - 1)$. But, if a and b are the roots of the polynomial $P(x)$ and $a - b \in R^*$ then $P(x)$ is divisible by $(x - a)(x - b)$.

We have an expansion $(x^p - 1)/(x - 1) = \prod_{i=1}^{p-1}(x - \gamma^{2i})$ by the choice of γ, then $p = \prod_{i=1}^{p-1}(1 - \gamma^i)(1 + \gamma^i)$. So, $\gamma^j - \gamma^l \in R^*$ when $j, l = 0, ..., p-1, j \neq l$.

Theorem 9: Let $\{s(t)\}$ be defined by (6), then $L = 2p$.

Proof: Let $L < 2p$, then there exists an associated connection polynomial $C(x)$ with degree less than $2p$ and

$$S(x)C(x) \equiv 0 \pmod{(x^{2p} - 1)}$$

by (15). According to Lemma 8 we can write: $C(\alpha^v) = 0$ for $v = 1, \ldots, 2p-1, v \neq p$. Then $C(x)$ is divisible by $(x^p - 1)/(x - 1)$, i.e., $C(x) = Q(x)(x^p - 1)/(x - 1)$, $Q(x) \in \mathbb{Z}_4[x]$ and $2Q(x) \neq 0$. Further, by definition $S(1) = 2$, consequently $C(1) \in \{0, 2\}$ and $Q(1) \in \{0, 2\}$, hence $Q(x) = (x-1)F(x) + q, q \in \{0, 2\}$ or

$$C(x) = (x^p - 1)F(x) + q(x^p - 1)/(x - 1).$$

Then, we obtain $2F(\alpha^v) = 0$ for $v = 1, 3, \ldots, 2p-1$, therefore $2F(x)$ is divisible by $x^p + 1$. Since the degree of $F(x)$ is less than p, we get a contradiction.

Consequently, $L = 2p$. ■

Lemma 10: Let the sequence $\{s(t)\}$ be defined by (7). Then $L = 2p$.

Lemma 10 we prove in the same way as Theorem 9.

V. Conclusion

We examined new quaternary sequences constructed on the cyclotomic classes of order four. We showed that they have high linear complexity and satisfactory autocorrelation. The linear complexity is derived over the finite field of order four and over the ring of four elements.

References

[1] T. W. Cusick, C. Ding, A. Renvall, *Stream Ciphers and Number Theory*, Amsterdam, Elsevier, 1998.

[2] C. Ding, T. Hellesenh, H. M. Martinsen, "New families of binary sequences with optimal three-level autocorrelation", *IEEE Trans. Info. Theory*, vol. IT-47, pp. 428–433, 2001.

[3] C. Ding, T. Helleseth, W.Shan, "On the linear complexity of Legendre sequences", *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276–1278, 1998.

[4] X. Du, Z. Chen Z, "Linear Complexity of Quaternary Sequences Generated Using Generalized Cyclotomic Classes Modulo $2p$, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*. vol. E94-A:5, pp. 1214–1217, 2011.

[5] V. A. Edemskii, "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes", *Discret. Math. Appl.*, vol. 20(1), pp. 75-84, 2010 (*Diskretn. Mat.*, vol. 22(1), pp. 74-82, 2010).

[6] D. H. Green, "Linear complexity of modulo-m power residue sequences", *IEE Proc., Comput. Digit. Tech.*, vol. 151(6), pp. 385–390, 2004.

[7] M. Hall, *Combinatorial Theory*, New York, Wiley, New York, 1975.

[8] P. Ke, S. Zhang,"New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity",*Inform. Proc. Letters*, vol. 112(16), pp. 646-650, 2012.

[9] Y. J. Kim, Y. P. Hong, H. Y. Song, "Autocorrelation of Some Quaternary Cyclotomic Sequences of Length $2p$", *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A:12, pp. 3679–3684, 2008.

[10] S. M. Krone, D. V. Sarwate, "Quadriphase sequences for spread spectrum multiple-access communication", *IEEE Trans. Inf. Theory*, vol. IT-30(3), pp. 520-529, 1984.

[11] H. D. Luke, H. D.Schotten, H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A survey", *IEEE Trans. Info. Theory*, vol. IT-49, pp. 3271–3282, 2003.

[12] H. Niederreiter, "Linear complexity and related complexity measures for sequences", *In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS*, vol. 2904, pp. 117. Springer, Heidelberg, 2003.

[13] A. Topuzoglu, A. Winterhof, "Pseudorandom sequences", *In: Garcia A., Stichtenoth H. (eds.) Topics in Geometry, Coding Theory and Cryptography, Algebra and Applications*, vol. 6, pp. 135-166. Springer-Verlag, Berlin, 2007.

[14] Z. X. Wan, *Finite Fields and Galois Rings*, Singapore, World Scientific Publisher, 2003.

[15] Z. X. Wan, *Algebra and Coding Theory*, Beijing, Science Press, 1976.